

IN THE CLAIMS

1. (Currently Amended) A person authentication system for executing person authentication by comparing a template which is person identification data acquired beforehand with sampling information input by a user, said system comprising: ~~an entity for executing person authentication, wherein said entity acquires a~~

an acquisition unit for acquiring an encrypted template from a person identification certificate storing ~~temperature~~ template information including said encrypted template and generated by a third-party agency serving as a person identification certificate authority;

a decrypting unit for decrypting said encrypted template; and

a person authenticating unit for executing ~~executes~~ person authentication ~~on the basis of the acquired~~ by comparing said decrypted template with said sampling information.

2. (Original) A person authentication system according to Claim 1, wherein the person identification certificate issued by said person identification certificate authority includes a digital signature written by said person identification certificate authority.

3. (Original) A person authentication system according to Claim 1, wherein said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued, acquires a template serving as person identification data of said person requesting the person identification certificate to be issued, and generates a person identification certificate storing template information including said template.

4. (Currently Amended) A person authentication system according to Claim 1, wherein, in the process of acquiring the person identification certificate from said person identification certificate authority, said ~~entity~~ person authentication system performs mutual authentication between said ~~entity~~ person authentication system and said person identification certificate authority, and said person identification certificate authority transmits the person identification certificate, provided that said mutual authentication is successfully completed.

5. (Original) A person authentication system according to Claim 1, wherein said person identification certificate authority stores said template in said person identification certificate after encrypting said template.

6. (Currently Amended) A person authentication system according to Claim 1, wherein said ~~entity~~ person authentication system is any one of a service provider which ~~makes a deal with~~ provides services to a user identified by said person identification certificate, a user device accessed by a user identified by said person identification certificate, and said person identification certificate authority.

7. (Currently Amended) A person authentication system according to Claim 1, wherein, when transmitting said person identification certificate to said ~~entity~~ person authentication system, said person identification certificate authority transmits a template which is stored in said person identification certificate, as an encrypted template which is decryptable only by said ~~entity~~ person authentication system to which said person identification certificate is to be transmitted.

8. (Currently Amended) A person authentication system according to Claim 1, wherein said ~~entity~~ person authentication system is a service provider which ~~makes a deal with~~ provides services to a user identified by said person identification certificate, and

wherein said service provider compares a template, which is acquirable from the person identification certificate acquired from said person identification certificate authority, with sampling information provided by the user and starts ~~making a deal with~~ providing services to the user, provided that said template and said sampling information match with each other.

9. (Currently Amended) A person authentication system according to Claim 1, wherein said ~~entity~~ person authentication system is a user device serving as a data processing apparatus including data accessible by a user identified by said person identification certificate, and

wherein said user device compares a template, which is acquirable from the person identification certificate acquired from said person identification certificate authority, with sampling information provided by the user, and said user device allows the user to start accessing said user device, provided that said template and said sampling information match with each other.

10. (Currently Amended) A person authentication system according to Claim 1, wherein said template is composed any one of: ~~biometric information of a person such as fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information;~~ non-biometric information ~~such as a seal, a passport, a driver's license, and a card;~~ any combination of two or more of said biometric information and said non-biometric information; and a combination of any of said information and a password.

11. (Currently Amended) A person authentication system according to Claim 1, wherein said ~~entity~~ person authentication system and said person identification certificate authority have an encryption processing unit, respectively, and

wherein, when data is transmitted therebetween, mutual authentication is performed between said ~~entity~~ person authentication system and said person identification certificate authority, a data-transmitting party generates a digital signature and adds it to data to be transmitted, and a data-receiving party verifies the digital signature.

12. (Currently Amended) A person authentication system for executing person authentication by comparing a template which is person identification data acquired beforehand with sampling information input by said person, said system comprising a person identification certificate authority which acquires an encrypted template from a person identification certificate storing template information including said encrypted template, decrypts said encrypted template, executes person authentication by comparing said decrypted template with said sampling information ~~on the basis of said acquired template~~, and issues a verification certificate, provided that said person authentication is successfully passed.

13. (Original) A person authentication system according to Claim 12, wherein the verification certificate issued by said person identification certificate authority includes a digital signature written by said person identification certificate authority.

14. (Original) A person authentication system according to Claim 12, wherein said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued, acquires a template serving as person identification data of said person requesting the person identification certificate to be issued, and generates a person identification certificate storing template information including said template.

15. (Currently Amended) A person authentication system according to Claim 12, wherein, in the process of acquiring the verification certificate from said person identification certificate authority, said ~~entity~~ person authentication system performs mutual authentication between said ~~entity~~ person authentication system and said person identification certificate authority, and said person identification certificate authority transmits the verification certificate, provided that said mutual authentication is successfully completed.

16. (Currently Amended) A person authentication system according to Claim 12, wherein said ~~entity~~ person authentication system acquiring the verification certificate is one of a service provider which ~~makes a deal with~~ provides services to a user identified by said person identification certificate, and a user device accessed by a user identified by said person identification certificate.

17. (Currently Amended) A person authentication system according to Claim 12, wherein said ~~entity~~ person authentication system acquiring the verification certificate is a service provider which ~~makes a deal with~~ provides services to an user, and

wherein said service provider starts ~~making a deal with~~ providing services to the user, provided that the verification certificate is successfully acquired from said person identification certificate authority.

18. (Currently Amended) A person authentication system according to Claim 12, wherein said ~~entity~~ person authentication system acquiring the verification certificate is a user device serving as a data processing apparatus including data accessible by an user, and

wherein said user device allows the user to start accessing said user device, provided that the verification certificate is successfully acquired from said person identification certificate authority.

19. (Currently Amended) A person authentication system according to Claim 12, wherein said ~~entity~~ person authentication system acquiring the verification certificate verifies the signature of said verification certificate acquired from said person identification certificate authority and deletes said verification certificate after confirming that said verification of the signature indicates the validity of said verification certificate.

20. (Currently Amended) A person authentication system according to Claim 12, wherein said template is composed any one of: biometric information ~~of a person such as fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information;~~ non-biometric information ~~such as a seal, a passport, a driver's license, and a card;~~ any combination of two or more types of said biometric information and said non-biometric information; and a combination of any of said information and a password.

21. (Currently Amended) A person authentication method for executing person authentication by comparing a template which is person identification data acquired beforehand with sampling information input by a user, said method comprising:

~~wherein an entity for executing person authentication acquires~~ acquiring an encrypted template from a person identification certificate storing template information including said

template and generated by a third-party agency serving as a person identification certificate authority;

decrypting said encrypted template;

comparing said decrypted template with said sampling information, and

~~executes~~ executing person authentication on the basis of the acquired template.

22. (Original) A person authentication method according to Claim 21, wherein said person identification certificate authority writes a digital signature on the person identification certificate issued by said person identification certificate authority.

23. (Original) A person authentication method according to Claim 21, wherein said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued, acquires a template serving as person identification data of said person requesting the person identification certificate to be issued, and generates a person identification certificate storing template information including said template.

24. (Currently Amended) A person authentication method according to Claim 21, wherein, in the process of acquiring the person identification certificate from said person identification certificate authority, said ~~entity~~ person authentication system performs mutual authentication between said ~~entity~~ person authentication system and said person identification certificate authority, and said person identification certificate authority transmits the person identification certificate, provided that said mutual authentication is successfully completed.

25. (Original) A person authentication method according to Claim 21, wherein said person identification certificate authority stores said template in said person identification certificate after encrypting said template.

26. (Currently Amended) A person authentication method according to Claim 21, wherein, when transmitting said person identification certificate to said ~~entity~~ person authentication system, said person identification certificate authority transmits a template which

is stored in said person identification certificate, as an encrypted template which is decryptable only by said ~~entity~~ person authentication system to which said person identification certificate is to be transmitted.

27. (Currently Amended) A person authentication method according to Claim 21, wherein said ~~entity~~ person authentication system is a service provider which makes a deal with a user identified by said person identification certificate, and

wherein said service provider compares a template, which is acquirable from a person identification certificate acquired from said person identification certificate authority, with sampling information provided by the user, and starts making a deal with the user, provided that said template and said sampling information match with each other.

28. (Currently Amended) A person authentication method according to Claim 21, wherein said ~~entity~~ person authentication system is a user device serving as a data processing apparatus including data accessible by a user identified by said person identification certificate, and wherein said user device compares a template, which is acquirable from a person identification certificate acquired from said person identification certificate authority, with sampling information provided by the user, and said user device allows the user to start accessing said user device, provided that said template and said sampling information match with each other.

29. (Currently Amended) A person authentication method for executing person authentication by comparing a template which is a person identification data acquired beforehand with sampling information input by a user, wherein, at a person identification certificate authority which acquires an encrypted template from a person identification certificate storing template information including said encrypted template, decrypts said encrypted template, and executes person authentication by comparing said decrypted template with said sampling information~~on the basis of said acquired template~~, a verification certificate is issued provided that said person authentication is successfully passed.

30. (Original) A person authentication method according to Claim 29, wherein said person identification certificate authority writes a digital signature on the verification certificate issued by said person identification certificate authority.

31. (Original) A person authentication method according to Claim 29, wherein said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued, acquires a template serving as person identification data of said person requesting the person identification certificate to be issued, and generates a person identification certificate storing template information including said template.

32. (Currently Amended) A person authentication method according to Claim 29, wherein, in the process of acquiring said verification certificate from said person identification certificate authority, said ~~entity~~ person authentication system performs mutual authentication between said ~~entity~~ person authentication system and said person identification certificate authority, and said person identification certificate authority transmits the verification certificate, provided that said mutual authentication is successfully completed.

33. (Currently Amended) A person authentication method according to Claim 29, wherein said ~~entity~~ person authentication system acquiring the verification certificate is a service provider which ~~makes a deal with~~ provides services to an user, and

wherein said service provider starts ~~making a deal with~~ providing services to the user, provided that the verification certificate is successfully acquired from said person identification certificate authority.

34. (Currently Amended) A person authentication method according to Claim 29, wherein said ~~entity~~ person authentication system acquiring the verification certificate is a user device serving as a data processing apparatus including data accessible by an user, and

wherein said user device allows the user to start accessing said user device, provided that the verification certificate is successfully acquired from said person identification certificate authority.

35. (Currently Amended) A person authentication method according to Claim 29, wherein said ~~entity~~ person authentication system verifies the signature of said verification certificate acquired from said person identification certificate authority and deletes said verification certificate after confirming that said verification of the signature indicates the validity of said verification certificate.

36. (Currently Amended) An information processing apparatus for executing person authentication by comparing a template which is person identification data acquired beforehand with sampling information input by a user, wherein an encrypted template is acquired from a person identification certificate generated by a third-party agency serving as a person identification certificate authority and storing template information including said encrypted template, the encrypted template is decrypted, and person authentication is executed by comparing said decrypted template with said sampling information ~~on the basis of the acquired template.~~

37. (Original) An information processing apparatus according to Claim 36, wherein the person identification certificate issued by said person identification certificate authority includes a digital signature written by said person identification certificate authority, and said information processing apparatus verifies the digital signature to check whether or not data has been tampered with.

38. (Original) An information processing apparatus according to Claim 36, wherein, in the process of acquiring a person identification certificate from said person identification certificate authority, said information processing apparatus performs mutual authentication between said information processing apparatus and said person identification

certificate authority, and said information processing apparatus receives the person identification certificate, provided that said mutual authentication is successfully completed.

39. (Original) An information processing apparatus according to Claim 36, wherein said information processing apparatus compares a template, which is acquirable from the person identification certificate acquired from said person identification certificate authority, with sampling information provided by the user, and said information processing apparatus starts performing a process requested by the user, provided that said template and said sampling information match with each other.

40. (Currently Amended) A program providing medium for providing a computer program which executes, on a computer system, a person authentication process for executing person authentication by comparing a template which is person identification data acquired beforehand with sampling information input by a user, said computer program comprising the steps of:

acquiring an encrypted template from a person identification certificate generated by a third-party agency serving as a person identification certificate authority and storing template information including said encrypted template;

decrypting said encrypted template; and

executing person authentication by comparing said decrypted template with said sampling information on the basis of said acquired template.